PRCA ИНТЕЛЕКТУАЛ ТИЗИМЛАР АСОСИДАГИ UZBCS БЛОКЧЕЙН КРЕДИТЛАШ ПЛАТФОРМАСИ УЧУН САМАРАЛИ ХЕШ ФУНКЦИЯ АЛГОРИТМИНИ ТАНЛАШ

Рахимбердиев Қ.Б.

Тошкент давлат иқтисодиёт университети

KALIT SO'ZLAR

Блокчейн технологияси, интеллектуал тизим, PRCA, хешлаш, хеш функция, оптималлаштириш, кредитлаш, UzBCS, майнинг, криптовалюта, криптографик алгоритм, очиқ калитли алгоритм,

ANNOTATSIYA

Ҳозирги вақтда блокчейн технологияси ахборотларни ҳимоялашнинг янги ва самарали технологияларидан бирига айланмоқда. Блокчейн технологияси криптовалюталарни яратиш, Internet of Thigs (IoT), хавфсиз молявий операцияларни амалга ошириш, соғлиқни сақлаш ва бошқа соҳаларда кенг қўлланилмоқда. Блокчейн криптобардошлиги юқори бўлган технология бўлишига қарамай, унда бир қанча хавфсизлик муаммолари аниқланмоқда. Жумладан, хеш функциялар блокчейн технологиясининг муҳим компоненти бўлиб, у бир томонлама функцияларга асосланади. Хавфсиз хешлаш жараёни асосан хеш функция алгоритми разрядлиги ҳамда хеш функцияда бажарилувчи мантиқий функциялар ва ҳисоблашларга боғлиқ. Хешлаш жараёни қанчалик тез амалга оширилса блокчейннинг майнинг самарадорлиги ортади. Шу сабабли мазкур ишда, PRCA (Proactive Reconfigurable Computing Architecture) интелектуал тизими асосида блокчейн хешлаш алгоритмини оптималлаштиришнинг янги схемаси таклиф этилади.

I.Кириш.

Блокчейн технологияси (инг. Blockchain – блоклар занжири) - бу маълум қоидалар асосида ишлаб чиқилган, маълумотларни сақловчи узлуксиз кетма-кетликдаги блоклар занжири [1; 2-5-б.]. Бошқача айтганда блокчейн, тақсимланган реестр технологияси (Distributed Ledger Technology, DLT) асосида ишлаб чиқилган.

Блокчейн технологияси дастлаб, Сатоши Накамото томонидан Bitcoin криптовалютасини яратишда қўлланилган. Кейинчалик унинг асосида, Litecoin, Monroe, Zcash, Ethereum каби бир қанча криптовалюталар ва уларнинг платформалари ишлаб чиқилди. Блокчейн технологияси жадал ривожланиши давомида маълумотларнинг ҳақийқийлиги ва ишончлилигини самарали таъминлаши ўз исботини топмоқда [1; 2-5-б. 2; 320-324-б.].

Шунинг билан бир қаторда, шахсга оид бўлган тиббий ва бошқа маълумотлар, ер мулк кадастри маълумотлари, шахслар еки ташкилотларнинг молявий маълумотларини ҳимоя қилиш ҳамда тақсимланган маълумотлар схемаларини ишлаб чиқишда кенг қўлланилиб келинмоқда. Блок, блокчейннинг асосий бирлиги бўлиб, дастлабки маълумотларни ўз ичига олувчи блок сарлавҳаси, манба маълумотлари ҳамда транзакция маълумотларини сақлайдиган блок танасидан иборат. Улар орасида блок сарлавҳаси маълумотлари олдинги блокни улаш ҳамда диапазон блокининг хеш қийматидан маълумотларни индекслашда фойдаланилади. Бунда, блокчейннинг ҳар бир транзакцияси, хеш функция билан ўзаро таъсири орқали амалга оширилади. Бу блокчейн ҳамда унинг асосида ишлаб чиқилган тизимлар хавфсизлигини кафолатлайди [3; 14757–14759-б.,4; 162-170-б., 5; 83-87-б.].

© *Рахимбердиев Қ.Б.*

Шу боис, блокчейн технологиясининг янада ривожланиши ва кўплаган соҳаларга тадбиқ қилинаётгани билан бир қаторда унинг хавфсизлик масалаларига катта эътибор қаратилмоқда. Ҳозирги кундаги илмий тадқиқотлари шуни кўрсатмоқдаки, блокчейн тизимларини шакллантиришда қўлланилаётган SHA1 хеш функцияси хавфсизлик жиҳатдан етарли дастурий – техник воситалар ҳамда ҳисоблаш ресурсларига бардошсиз бўлиши мумкин. Шу боис, хеш фукнция алгоритмларини янада такомиллаштириш, блокчейн тизимларида навбатдаги блок транзакция маьлумотларига мос бўлган оптимал хеш функция алгоритмини танлаш мақсад қилинади. Ушбу мақсадга эришиши учун блокчейн учун қўлланилаётган хеш функция алгоримини оптималлаштириш, ҳисоблаш вақтини камайтирган ҳолда ҳисоблаш тезлигини ошириш орқали амалга оширилади. Блокчейн учун динамик равишта хеш функцияларни танлаш масаласини ҳал қилишда PRCA (Proactive Reconfigurable Computing Architecture) механизмларидан фойдаланиш зарурли ва етарли ҳисобланади.

II.Адабиётлар таҳлили.

Бутун дунёда банк ва молиявий тизимларни такомиллаштириш замонавий FinTech (Financial technology-молиявий технология) технологиялар қўлланилиб келинмоқда. Ушбу молиявий технологиялар ахборот хавфсизлиги, иқтисодий хавфсизлик ва тезкор транзактцияларни бажариш имконини берувчи технологиялардан бири блокчейн технологияси ҳисобланади. Блокчейн технологияси дастлаб Сатоши Накамото томонидан амалиётга қўлланилган бўлиб, унинг "Bitcoin: A Peer-to-Peer Electronic Cash System" илмий мақоласида молиявий блокчейн архитектураси, тармоқ тузилиши, транзакцияларни яратиш жараёни, криптовалюта тузилиши ва ахборотларни химоялаш усуллари келтирилган.

Блокчейн технологияси бир қанча криптографик алгоритмларни ўз ичига олади. Хеш функция ва электрон рақамли имзо алгоритмлари ва ҳ.казолар шулар жумласидандир. Ушбу криптографик алгоритмларнинг асосий ғоялари ва модификация қилиш усуллари Б.Шнайернинг "Прикладная криптография" асарида келтирилган. Маьлумотлар яхлитлигини таьминлашда блокчейн технологиясини қўллаш бўйича Қ. Лу, Х. Ху, Қ. Хиа, Э. Б. Сифаҳ, К. О. Асамоаҳ, Ж. Гао, Х. Ду, М. Guizani илмий ишларида кузатишимиз мумкин.

Шунингдек, С. Х. Хи, W. Н. Зҳанг, Қ. Л. Зҳоу, С. ХуеМинг, ва Б. Ли ларнинг илмий ишларида миметик компютерлар учун SHA512 хеш функция алгоритмини такомиллаштириш натижасида юқори ҳисоблаш ва ўтказувчанлик самарадорлигига эришиш усуллари келтирилган. Ҳозирда блокчейн платформалари тобора оммолашаётганлиги сабабли унга бўлиши мумкин бўлган таҳдидларни бартараф этиш ва юқори самарадорликка эришишнинг янги усуллари тадқиқ қилинмоқда. Ушбу тадқиқодлардан бири, блокчейн платформалари учун қайта конфигурация қилинувчи компютер архитектурасини такомиллаштириш ҳисобланади. А.С. Беск ва бошқалар, К. Compton ва бошқалар илмий ишларида динамик қайта конфигурация қилинадиган компютер архитектураси ва уларни оптималлаштириш усуллари ҳамда дастурий воситаларини ишлаб чиқиш бўйича кўрсатмалар келтирилган бўлиб, улардан фойдаланиш самарали ҳисобланади.

III.Тадқиқод методологияси.

Ушбу илмий тадқиқод давомида, анализ, синтез, импирик, стохастик ва бошқа илмий тадқиқод методологияларидан фойдаланилган. Шунингдек, оқимли ва очиқ калитли криптографик моделлар ҳамда уларни самарадорлиги аниқлаш усуллари кўриб чиқилган.

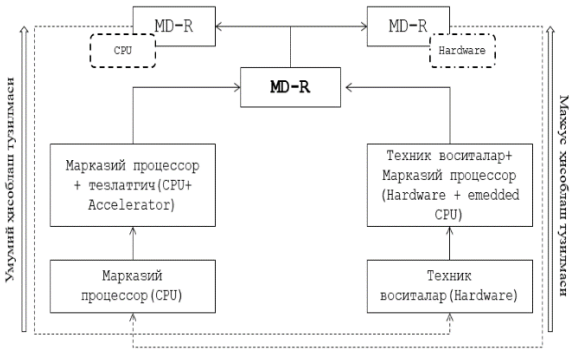
IV.Таҳлил ва натижалар

Проектив қайта конфигурация қилинувчи ҳисоблаш архитектураси. PRCA кўп ўлчамли қайта қурилувчи функционал тузилишга ҳамда динамик кўп танага асосланган операцион механизм бўлиб ҳисобланади. Проектив қайта конфигурация қилинувчи ҳисоблаш механизми маьлумотларни қайта ишлаш жараёнида, унинг ҳисоблаш, сақлаш ҳамда ўзаро боғланиш каби

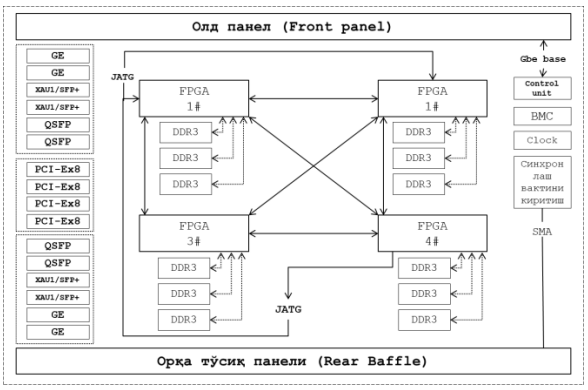
(cc) BY © *Рахимбердиев Қ.Б.*

бажарувчи тузилмалари асосий аппаратни ўзгартирмасдан операция самарадорлигини ошириш учун алгоритмни яхшилаш ҳамда транзакцияларни қайта ишлашда динамик равишта ўзгариб туради. PRCA механизмида кўплаб функционал эквивалентлар мавжуд бўлиб, улар ҳар хил аппарат тузилмаларни ушбу алгоритм билан бириктириш орқали амалга оширилади. PRCA механизмини қўллашда, ҳисоблашнинг юқори кўрсаткичларига эришиш, яъни оптимал ҳисоблаш мажмуасини яратиш учун ўзгарувчиларни автоматик қабул қилиш ҳамда қайта ишлаш алгоритмида ҳисоблаш жараёнини автоном тарзда қайта қуриш мақсад қилинган[6; 76-80-б.].

PRCA механизми ҳар хил масалаларнинг оптимал ечимларини олишга имконият берувчи ўзгарувчан инфраструктура ҳамда алгоритмни ўз ичига олади. Механизм ҳар хил тизим юкламалари ёки бошқа ҳолатларда энг мос бўлган маьлумотларни қайта ишлаш компонентларини ҳамда тизим учун энг мос бўлган архитектурани шакллантирган ҳолда кенг қамровли юқори самарадорликка интилади, Проектив қайта конфигурацияланадиган ҳисоблаш, масалаларни самарали ҳал қилиш учун, масалани ечишнинг умумий ҳамда махсус ҳисоблаш усулларининг афзалликларини бирлаштирган ҳолда амалга оширади. Умумий ҳисоблаш тузилмаси нуқтаи назаридан, у масалага мос бўлган аниқланган тузилмалари ҳамда ўзгарувчан алгоритми билан тавсифланади. Натижада, ихтиёрий масалани юқори самарадорлик билан ҳисоблаши мумкин.



1-расм. Проектив қайта конфигурация қилинувчи ҳисоблаш архитектураси



2-расм. Проектив қайта конфигурация қилинадиган компютер архитектураси

Проектив қайта конфигурация қилинувчи компютер-ҳисоблашнинг юқори самарадорлигига эришиш учун миметик ҳисоблаш принципига мувофиқ ишлаб чиқилган янги турдаги компютер. Миметик ҳисоблаш машинасининг ҳисоблаш тузилмаси, юқори тартибли функция сифатида қаралиши мумкин. ПҚККҚ ихтиёрий ҳисоблаш тизимини таҳлил қилиш учун, суньий интелект алгоритми орқали ўзгарувчиларни мустақил танлайди ҳамда самарали бўлган ҳисоблаш тузилмалари тўпламини яратади. Бунда, ПҚККҚ нинг асосий моҳияти, у ҳисоблаш тузилмаларини функционаллаштиради.

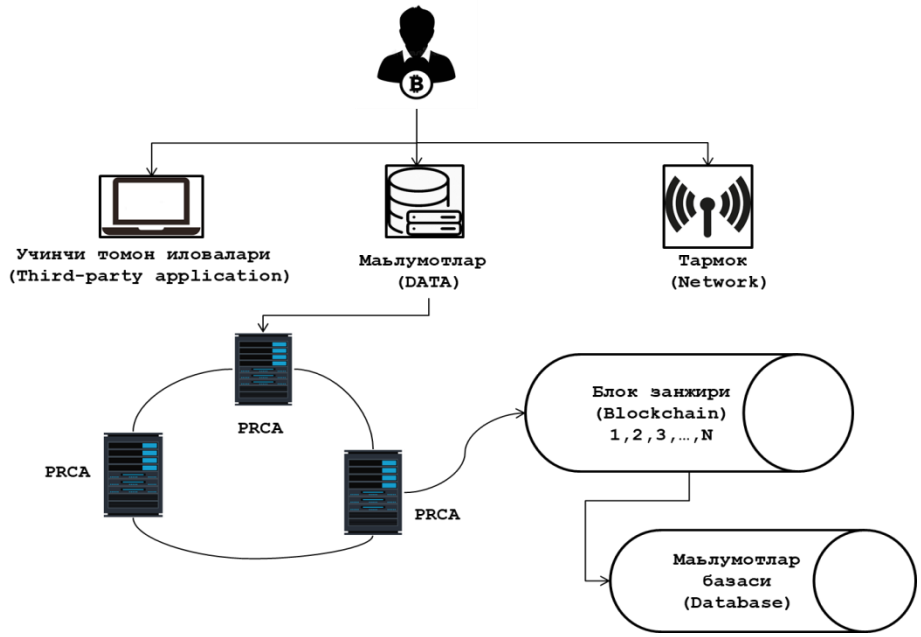
Проектив қайта конфигурация қилинадиган компютердан асосан интенсив ҳисоблашларни бажаришда фойдаланилади. Мазкур компютер АТОМ умумий микропроцессори, тўртинчи тартибли қайта конфигурация қилинадиган ҳамда кенг қамровли қайта конфигурация қилинувчи FPGA ва DDR3 тезкор ҳотирадан иборат бўлиб, у LVDS шинасини ҳамда FULL-MESH қатламини GTX қўшимча график платалари орқали боғлаган ҳолда BMC бошқарув блоки томонидан бошқарилади. Шунингдек, вақт синхронизацияси блоки орқали синхронланади (2-расм).

PRCA асосида хеш функция алгоритмларини оптималлаштириш ва блокчейн хавфсизлик самарадорлигини ошириш. PRCA блокчейн тармоғининг тугуни сифатида созланиши мумкин. Блокчейн тармоғида PRCA ҳамда фойдаланувчилар ўртасида алоқа ўрнатилади. PRCA маьлумотларни DDR хотирасида сақлайди

(cc) BY © *Рахимбердиев К.Б.*

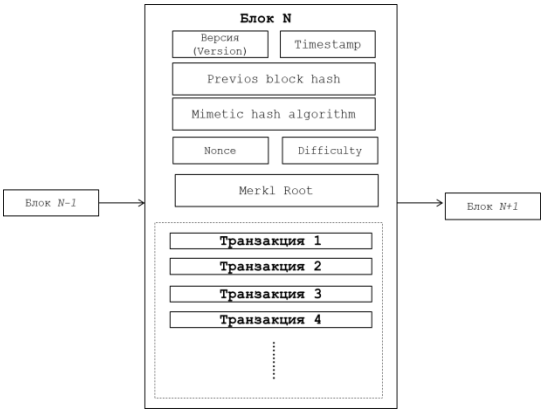
ҳамда асинхрон FIFO методи орқали тармоқдан хотира маълумотларига юқори тезликдаги тўғридан – тўғри уланиш бажарилади[8; 57-66-б.].

Конвейрда хеш қийматлар ҳисобланган сўнг натижа инкапсуляция қилинади, яъни ҳисобланган хеш қиймат натижалари ўзгартирилиши дастур томонидан тақиқлаб қўйилади. Жараён сўнгида блокчейн сақлашни якунлаш учун сақлаш серверига юборилади ҳамда маълумотлар базага сақланади. Мазкур тизимнинг умумий кўриниши 3-расмда келтирилган.



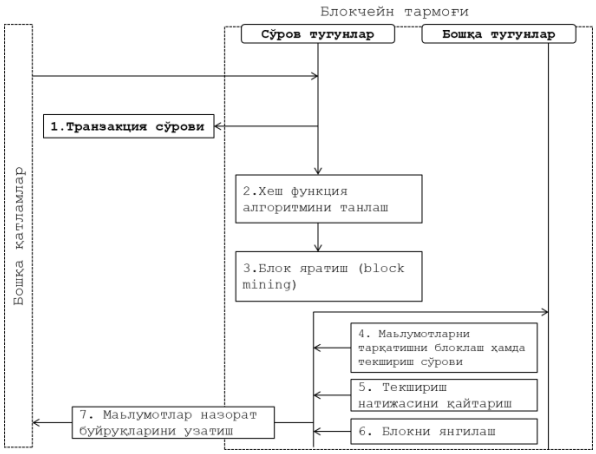
3-расм. PRCA асосида хеш функция алгоритмларини оптималлаштириш ва блокчейн хавфсизлик схемаси

Блок, блокчейннинг асосий бирлиги бўлиб, у транзакциялар тўғрисидаги барча маълумотларни, транзакция яратилиш вақти, транзакция ёзувининг тартиб рақами, транзакцияларнинг хеш қийматлари, унинг чиқимлар адреси ҳамда миқдори (биткоин криптовалютаси мисолида) ва бошқа турдаги маълумотларни ўз ичига олади. Транзакцияларда Меркл дарахти қиймати ҳисобланади ва ушбу хеш қиймат Merkl Root деб аталади. Merkl Root қиймати ҳар бир транзакция хеш адресини қайта сотиш ва қалбакилаштириш мумкин эмаслигини ифодалайди. Энди биз транзактциялар хавфсизлигини янада такомиллаштириш мақсадида блокчейнга проектив қайта конфигурация қилинадиган хеш функция пакетини қўллаймиз, ушбу пакет хеш функция алгоритмоарининг ҳар хил турлари ва тузилмаларидан иборат бўлади. Улар блокчейнда алоҳида ёки интелектуал тизим танловига биноан ишлаши мумкин. Проектив қайта конфигурация қилинадиган блокчейннинг блок тузилиши 4-расмда келтирилган.



4-расм. Проектив қайта конфигурация қилинадиган блокчейннинг блок тузилиши

© Рахимбердиев К.Б.



5-расм. Блок майнинги ва янгилашнинг умумий схемаси

Блокчейндаги бирлик тугунлар транзакция ҳажмини ҳисоблаш учун тармоқ трафигини кузатиб боради. Транзакция яратилмасдан олдин оптимал хеш функция алгоритмини танлаш босқичи бажарилади, сўнгра хеш функция рўйҳатидан оптимал бўлган хеш функция алгоритми танланади. Бирлик тугунларнинг хеш қийматини ҳисоблашда майнерлар танланган хеш функциядан фойдаланади. Хеш қиймат ҳисобланган блокчейннинг консенсус алгоритмлари ишга тушади. Блокни текшириш учун ҳисобланган хеш қиймат блокчейндаги барча тугунларга тарқатилади [9; 29-32-б.].

Ўзаро муносабат ҳолатида сенсор қатлам блокчейн маълумотларини йиғади.Сенсор маълумотларни бирлик тугунларга юборади ҳамда маълумотларни сақлаш учун транзакцияни сўрайди. Агарда бирлик тугунлар транзакцияни майнинг қилишни мувофаққиятли якунласа, блокчейн тармоғи блокни янгилайди. Шундан кейин, блокчейн тармоғи майдон қатлами маълумотларини бошқарув қатламига қайтаради. Кейин яна блок майнинг қилиш жараёни амалга оширилади. Блок яратиш жараёни якунланган сўнг, блокчейн тармоғи транзакция тугунини қабул қилади ҳамда бошқа тугунларга блокни текшириш сўровини юборади. Текшириш сўровини блок сарлавҳасидаги хеш қиймат ҳисобланган хеш функция алгоритмларига эга бўлган блокчейн тугунлари қабул қилади. Блокни текшириш жараёни мувофаққиятли якунлангандан сўнг блок янгиланади (5-расм).

Шунингдек, тасодифий сонлар генераторидан фойдаланган ҳолда янги хеш функция алгоритми интервали танланади ҳамда томонлар хафвсизликни яхшилаш мақсадида келтирилган интервалдан хеш функция алгоритмини келишган ҳолда танлаб олишади.

1.2.SHA256 хеш функция алгоритми.

Рақамли алоқа тизимлари турли хил электрон операцияларни амалга ошириш учун кенг қўлланилади. Жумладан, электрон молявий хизматлар, электрон ўтказмалар, мобил алоқа, мултимедиа, электрон тижорат, алоқа каналлари орқали ҳужжатлар алмашинуви, видеоконференциялар ва бошқалар. Ушбу алоқа тизимлари орқали амалга ошириладиган ахборот алмашинуви жараёнида хафвсизлик чораларига эътибор берилмаса, мазкур тизимлар орқали узатиладиган маьлумотларга турли хил хавфлар бўлиши мумкин. Очиқ алоқа каналларида узатиладиган маьлумотларга бўлиши мумкин бўлган хавфлар қуйидагича тавсифланади:

- Тизимга руҳсатсиз кириш
- Хизмат кўрсатишни рад этиш
- Маьлумотлар конфеденциалиги бузилиши
- Маьлумотлар сизиб чиқиши
- Тизим мониторинг ҳужумлари
- Аутентификация ва идентификацион хужумлар

Бу каби бўлиши мумкин бўлган хавфларни камайтириш мақсадида бир қатор тизимли хавфсизлик чораларини кўриш мумкин. Жумладан, брандмауэрларни фойдаланиш, трафикни филтрлаш ҳамда хавфларни аниқлаш тизимлардан фойдаланиш самарали натижаларга олиб келади. Шунингдек, тизимлар хавфсизлигини криптографик воситалар орқали ишончли тарзда ҳимоялаш мумкин [10; 334-336-б.].

Хеш функциялар кўплаган криптографик алгоритмларнинг ажралмас қисми ҳисобланади. Хеш функцияларни қўллаш учун бир нечта алгоритмлар таклиф қилинган: MD5, SHA-1, SHA-2, Whirlpool, Haval ҳамда RipeMD-160 алгоритмларидар. Ҳозирги вақда

(cc) BY © Рахимбердиев К.Б.

хеш функциялар устида олиб борилган илмий тадқиқотлар шуни кўрсатмоқдаки MD5 ва SHA оиласига мансуб бўлган алгоритмлар хавфсизлик талабларига юқори даражада жавоб беради [11; 6-7-б.].

Шу боис, бу хеш функциялар оиласига мансуб бўлган алгоритмлар авлодларини соҳаларда хавфсиз маълумотлар алмашинувини амалга оширишда кенг қўлланилмоқда. Масалан, Биткоин, Эфиреум, Литекоин ва бошқа криптовалюталарда транзакциялар хавфсизлиги ҳамда аутентификация масалалрини ҳал қилишда SHA (Secure Hashing Algotihm) оиласига мансуб бўлган қуйидагича алгоритмлар қўлланилади (1-жадвал) [12; 7-8-б.].

1-жадвал.

SHA (Secure Hashing Algorithm) алгоритмларнинг ўлчами ва хавфсизлик хусусиятоарининг битларда акс эттирилиши

Хеш функция алгоритмлари	*SHA-1*	*SHA-256*	*SHA-384*	*SHA-512*
Хабар ўлчами	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Блок ўлчами	*512*	*512*	*1024*	*1024*
Ёзув ўлчами	*32*	*32*	*64*	*64*
Хабар дайджеси ўлчами	*160*	*256*	*384*	*512*
Хавфсизлик	*80*	*128*	*192*	*256*

1-жадвалда келтирилган SHA оиласига мансуб бўлган хеш функция алгоритмлари блокчейн тизимларини ишлаб чиқишда жуда муҳим бўлган механизмлар бўлиб, улар битларда, ички мантиқий функциялар, кирувчи хабар ҳажми, хабар блоки ўлчами, хабар сўзлари ўлчами, хавфсизлик ўлчовлари ҳамда хабар дайджеси ўлчамлари билан бир биридан фарқ қилади. Лекин, ушбу алгоритмлар функционал бажарилиши жиҳатдан бир хил амалга оширилади[13; 543-547-б.].

Хеш функциялар блокчейн технологиясининг муҳим компоненти бўлиб, у кўплаб операцияларни бажаришда қўлланилади. Хешлаш – бу маълум бир турдаги ва ихтиёрий узунликдаги кириш маълумотлари массивини фиксирланган узунликдаги чиқувчи битлар қаторига (бутун сон) айлантириш. Бундай акслантириш (айлантириш) хеш-функсия деб ҳам аталади.

Хешлаш ассоциатив массивларни ташкил қилиш учун қўлланилади, бунда индекслари сонлар емас, балки ихтиёрий қийматлар бўлади. Хешлашдан одатда матнлардан нусхаларнинг такрорланишини қидиришда, яъни хеш-функсияларининг бир хил қийматига эга бўлакларни қидиришда фойдаланилади. Бундан ташқари, хешлаш кўпинча паролларни сақлаш учун ишлатилади.

Шунинг билан биргаликда ноёб идентификаторларни яратиш учун, масалан, агар файл ўзига хос номни талаб қилса, сиз ушбу файлни хешлаш натижасини ҳисоблаб чиқишингиз ва натижани файлга ном сифатида ишлатишингиз мумкин. Шунингдек, бу матнларнинг назорат суммасини ҳисоблаш учун жуда муҳимдир. Айтайлик, фойдаланувчи тармоқ орқали бир нечта матн юбориши керак. Текшириш суммаси матн билан бирга узатилади, олинганидан кейин асл нусхаси билан текширилади. Агар суммаси мос келмаса, демак матнни узатишда қандайдир хатолик бўлганлиги ҳақида хулоса қилиш мумкин бўлади.

Бироқ, кўпинча киришдаги турли узунликдаги бир нечта турли хил маълумотлар, чиқишда бир хил маълумотларга мос келиши мумкин. Турли хил маълумотлар бир ҳил хеш қийматига эга бўлган ҳолатлар коллизия (тўқнашув) деб аталади. Бундай ҳолда, хешлаш алгоритми ҳар хил маълумотларнинг ҳар хил қийматга ега бўлишини таъминлашга интилиши керак. Камдан кам ҳолларда коллизияларнинг олдини олиш мумкин.

Хешлаш жараёни электрон ҳисоблаш машинаси ҳамда алгоритмда бажариладиган ҳисоблашларга боғлиқ турда белгиланган узунликда ва вақтда бажарилади. Хешлаш жараёнинг самарадорлигини ошириш учун хеш функция алгоритмини оптималлаштириш талаб қилинади. Проектив қайта конфигурация қилинадиган компютерларда хеш функцияларни оптималлаштиришни SHA256 алгоритми мисолида қуйидагича кўриб чиқамиз.

(cc) BY © *Рахимбердиев К.Б.*

SHA256 хеш функция алгоритми узунлиги 2^{64} битдан ошмайдиган хабарлар учун 256 бит узунликдаги хеш қийматни ҳисоблайди ва бу қиймат хабар дайджеси деб аталади. Хабар дайджеси 32 байтли массив бўлиб, узунлиги 64 та ўн олтилик саноқ системасидаги қатор кўринишида ифодаланади. Мазкур хешлаш алгоритми икки қисмдан иборат бўлиб, зичлаш функцияси ҳамда маълумотларни қайта ишлаш алгоритмларига бўлинади.

Зичлаш функцияси 256 бит узунликдаги оралиқ хеш қийматни, матннинг навбатдаги блокини калит сифатида фойдаланган ҳолда шифрлаш алгоритмидан иборат бўлади. Зичлаш функциясида асосий амаллардан ташқари қўшимча равишта силжитиш амаллари қўлланилади. Бунда, R^n - ихтиёрий сўзни n бит ўнгга силжитиш, S^n - ихтиёрий сўзни n бит ўнгга циклик силжитишни билдиради. Алгоритмда кирувчи сўзнинг ўлчами 32 битга тенг қилиб олинади ва қўшиш амали 2^{32} модули бўйича бажарилади. Дастлабки ҳисоблашларда, $H^{(0)}$ бошланғич хешлаш вектори танланади. Ушбу бошланғич вектор 32 разрядли 8 та сўзлардан иборат бўлиб, у қуйидагича туб сонлар квадрат илдизи қийматининг каср қисмларига тенг бўладигандай қилиб олинади.

$$H^{(0)} = \{6a09e667,\ bb67ae85,$$
$$3c6ef372,\ a54ff53a,$$
$$510e527f,\ 9b05688c,$$
$$1f83d9ab,\ 5be0cd19\}.$$

SHA256 алгоритми қуйидагича бажарилади.

Кенгайтирилган қайта ишлаш. Хешлаш лозим бўлган маълумот SHA-1 алгоритми каби узунлиги 512 битга каррали бўлгунча тўлдирилади. Дастлабки тўлдириш жараёнидан сўнг маълумот қаторига 1 ёзилади ҳамда қолган битлар ноллар билан қайта тўлдирилади. Бунда, маълумот узунлиги 512 модули бўйича таққослама бажарилиши зарурли ва етарли. Кейинчалик, маълумотнинг 64 битлик узунликдаги қаторлари ёзилади.

Кирувчи маълумотни 512 битлик блокларга ажратиш. 512 битли кенгайтирилган маълумот 32 битлик $M^{(1)}, M^{(2)}, ..., M^{(k)}$ блокларга ажратилади. SHA256 алгоритмида ҳар бир блок бу 16 та блокни ташкил қилади. Яъни, $M^{(1)}, M^{(2)}, ..., M^{(16)}$.

Ўзгарувчиларни инициализация қилиш. $K_0, ..., K_{63}$ ўзгармас қийматлар сифатида 64 та 16 лик саноқ системаси кўринишида тасвирланган туб сонлар куб илдизи каср қисмларининг биринчи 32 бити олинади. Шунингдек, A, B, C, D, E, F, G, H регистрларни хеш функциянинг $H_0^{(t-1)}, ..., H_7^{(t-1)}$, $(t-1)$ оралиқ қиймати билан қуйидагича инициализация қилинади.

$$A = H_0^{(t-1)}, B = H_1^{(t-1)}, C = H_2^{(t-1)},$$
$$D = H_3^{(t-1)}, E = H_4^{(t-1)}, F = H_5^{(t-1)}, \quad (3)$$
$$G = H_6^{(t-1)}, H = H_7^{(t-1)},$$

Асосий бажарилувчи цикл. Мазкур хеш функция алгоритмида аргументи ҳамда қийматлари 32 бит бўлган қуйидагича мантиқий функциялардан фойдаланилади.

$$CH(E_t, F_t, G_t) = (E_t \wedge F_t) \oplus (E_t \wedge G_t) \quad (4)$$

$$Maj(A_t, B_t, C_t) = (A_t \wedge B_t) \oplus (A_t \wedge C_t) \oplus (B_t \wedge C_t) \quad (5)$$

$$\sum_0 (A_t) = S^2(A_t) \oplus S^{13}(A_t) \oplus S^{22}(A_t) \quad (6)$$

$$\sum_1 (E_t) = S^6(E_t) \oplus S^{11}(E_t) \oplus S^{25}(E_t) \quad (7)$$

$$\delta_0(H_t) = S^7(H_t) \oplus S^{18}(H_t) \oplus R^3(H_t) \quad (8)$$

$$\delta_1(D_t) = S^{17}(D_t) \oplus S^{19}(D_t) \oplus R^{10}(D_t) \quad (9)$$

Энди, A, B, C, D, E, F, G, H регистрлари учун зичлаш функциялари қуйидагича қўлланилади. Бунда, зичлаш функцияси t ўзгарувчисининг $0 \le t \le 63$ ораликдаги (4) формулада берилган мантиқий функциялар қийматларидан фойдаланган ҳолда ҳисобланади.

© Рахимбердиев К.Б.

$$T_{t+1} = H_t + \sum_1(E_t) + \sum_0(A_t) + CH(E_t, F_t, G_t) + Maj(A_t, B_t, C_t) + W_t + K_t \quad (10)$$

$$L_{t+1} = H_t + \sum_1(E_t) + CH(E_t, F_t, G_t) + W_t + K_t + D_t \quad (11)$$

Бунда,

$\sum_1(E_t)$, $\sum_0(A_t)$, $CH(E_t, F_t, G_t)$, $Maj(A_t, B_t, C_t)$ - (4) формулада келтирилган мантиқий функциялар,

W_t -зичлаш функцияси

K_t -ўзгармас қийматлар (SHA256 хеш функция алгоритми учун 64 та 16 лик саноқ системаси кўринишида тасвирланган туб сонлар куб илдизи каср қисмлари)

H_t- кирувчи маьлумотлар ажратилган регистр

Шунингдек, Кенгайтирилган $M^{(k)}$ маьлумот 512 битлик $M^{(k)} = M_0^{(k)}, M_1^{(k)}, \ldots, M_{15}^{(k)}$ блокларга ажратилади ҳамда $W_0, W_1, ..., W_{63}$ зичлаш функцияси қийматлари қуйидагича ҳисобланади.

$$W_t = \begin{cases} M_t^{(k)} \\ \sigma_1\left(W_{(t-2)}\right) + W_{(t-7)} + \sigma_0\left(W_{(t-15)}\right) + W_{(t-16)} \end{cases} \quad (12)$$

Бунда,

$\sigma_1\left(W_{(t-2)}\right)$, $\sigma_0\left(W_{(t-15)}\right)$ - силжитиш ҳамда циклик силжитиш амалларини бажарувчи мантиқий функциялар.

Ҳисоблашларнинг ҳар бир итерацияси бажарилгандан сўнг $A_t, B_t, C_t, D_t, E_t, F_t, G_t, H_t$ регистрлари қийматлари янгиланади:

Яьни,

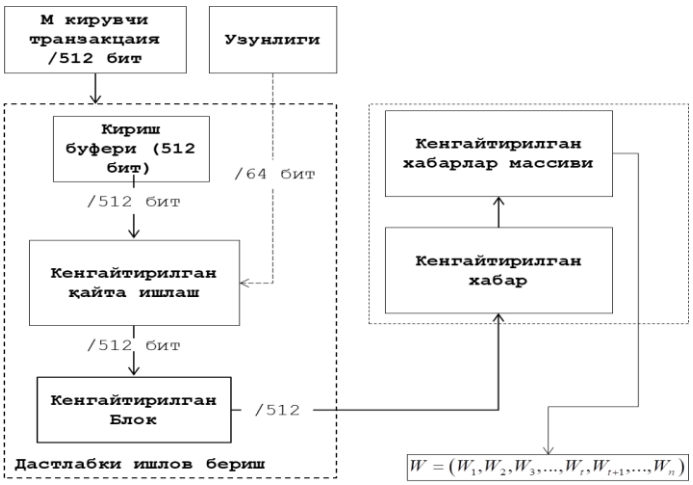
$$H_{t+1} = G_t, G_{t+1} = F_t, F_{t+1} = E_t,$$
$$E_t = T_{t+1} + D_{t+1}, D_{t+1} = C_t, \quad (13)$$
$$C_{t+1} = B_t, B_{t+1} = A_t, A_{t+1} = A_{t+1} + L_{t+1}$$

Регистр қийматларини янгилаш жараёнидан кейин, t - оралиқ хеш қиймат $H^{(t)}$ қуйидагича ҳисобланади.

$$\begin{aligned} H_0^{(t)} &= A_{t+1} + H_0^{(t-1)} \\ H_1^{(t)} &= B_{t+1} + H_1^{(t-1)} \\ H_2^{(t)} &= C_{t+1} + H_2^{(t-1)} \\ H_3^{(t)} &= D_{t+1} + H_3^{(t-1)} \\ H_4^{(t)} &= E_{t+1} + H_4^{(t-1)} \\ H_5^{(t)} &= F_{t+1} + H_5^{(t-1)} \\ H_6^{(t)} &= G_{t+1} + H_6^{(t-1)} \\ H_7^{(t)} &= H_{t+1} + H_7^{(t-1)} \end{aligned} \quad (14)$$

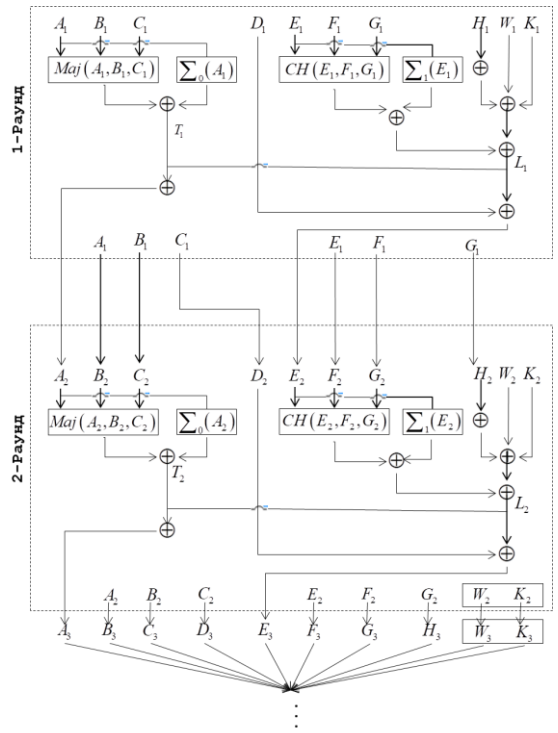
V.Натижа.

Натижада, $H^{(N)} = H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$ ифода M маьлумотнинг хеш қийматини беради. SHA 256 хеш функция алгоритми бўйича такомиллаштирилган қуйидагича схемаси таклиф этилади.

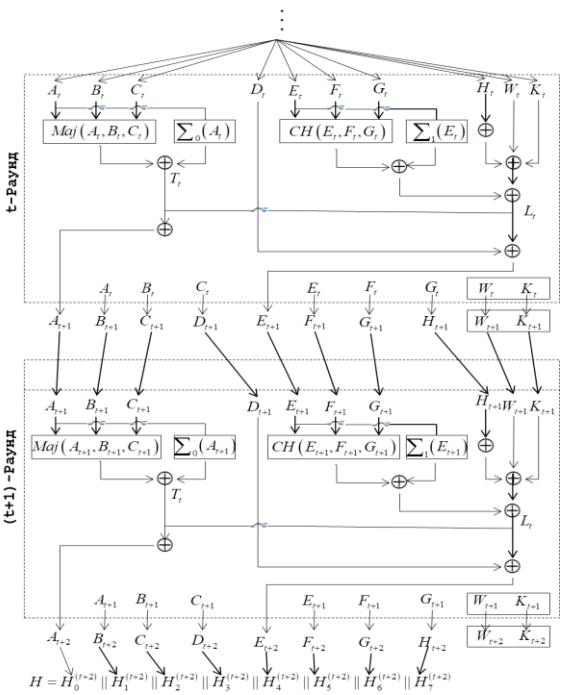


7-расм. SHA 256 хеш функция алгоритмининг кенгайтирилган қайта ишлаш жараёни

© Рахимбердиев К.Б.



8-расм. Хеш қийматни ҳисоблашда бажариладиган 2 раундли итерацион жараён схемаси



9-расм. Хеш қийматни ҳисоблашда бажариладиган $(t+1)$ раундли итерацион жараён схемаси

7-8-9-расмларда SHA 256 алгоритми бажарилишининг барча босқичлари келтирилган. Бу алгоритм схемасидан фойдаланган ҳолда иҳтиёрий кирувчи транзакция хабарини хешлаш мумкин. Транзакцияларни хешлаш жараёни самарадорлигини аниқлаш учун алгоритмда бажарилувчи амалларни таҳлил қилишимиз зарур. Қуйида 512 битлик хабар блоки учун ҳисобланадиган мантиқий функцияларнинг 64 та итерацияда бажариладиган барча операциялари ҳамда қатор оҳирида бажарилувчи 8 сўзни қўшиш амаллари келтирилган.

VI.Хулоса.

Блокчейн технологияси юқори ҳисоблаш мураккаблигига эга бўлган криптографик ва бошқарув алгоритмларини ўз ичига олади. Шу боис, блокчейн платформалари учун самарали ҳисоблаш воситаларини лойиҳалаш талаб этилади. Проектив қайта конфигурация қилинувчи компютер шу каби ҳисоблаш воситаси лойиҳаси бўлиб, у аньанавий компютердан асосий афзаллиги ҳисоблаш жараёнини амалга ошириш учун 10 баробар кам энергия сарф қилади.

Ушбу компютерлар ахборот хавфсизлигини таьминлашда асимметрик ҳимоялаш алгоритмларидан фойдаланади. Мазкур хавфсизлик тизимларини қуришда динамик тасодифийликдан фойдаланилади. Бу ҳусуият крипто аналитиклар томонидан англаниши ҳамда ички ҳужумларни камайтириш мақсадида ҳужум қилинувчи сиртни кенгайтиради. Компютернинг келтирилган ҳусусиятларига асосланган ҳолда, маьлумотларни узатишдаги кечикишларни камайтириш, симулацион хеш тузилмаларни яратиш ҳамда FPGA ёрдамида блокчейн маьлумотларининг хеш қийматини ҳисоблаш тезлигини 10000 Мбит/с гача оширишга имконият беради.

VII.Адабиётлар рўйҳати.

1. Nakamoto, Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System (24 мая 2009).
2. Nakamoto, Satoshi Bitcoin P2P e-cash paper (31 октября 2010).
3. Q. Lu and X. Xu, "Adaptable blockchain-based systems: a case study for product traceability," IEEE Software, vol. 34, no. 6, pp. 21–27, 2017.

© Рахимбердиев К.Б.

4. M. Padmavathi and R. M. Suresh, "Secure P2P intelligent network transaction using Litecoin," Mobile Networks and Applications, vol. 24, no. 2, pp. 318–326, 2018.
5. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, no. 99, pp. 14757–14767, 2017.
6. G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 162–173, 2019.
7. S. X. Xi, W. N. Zhang, Q. L. Zhou, S. XueMing, and B. Li, "High-throughput implementation of SHA512 algorithm based on mimetic computer," Computer Engineering and Science, vol. 40, no. 8, pp. 1344–1350, 2018.
8. A.C.S. Beck *et al.* Dynamic Reconfigurable Architectures and Transparent Optimization Techniques ACM. (2010).
9. K. Compton et al.Reconfigurable computing: a survey of systems and softwareACM Comput. Surv.(2002).

© *Рахимбердиев К.Б.*